

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
Great Falls Division**

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
STMARTINSCHURCH091@GMAIL.COM
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE, INC.

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Shiloh A. Allen, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, Inc. (Google), an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since April 13, 2008. Currently, I am assigned to the Cyber Crime Squad of the Salt Lake City, Utah Field Office. My experience as an FBI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of fraud and intrusion. I have received training and gained experience in interviewing and interrogation techniques, arrest

procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment as well as interview and interrogation of subjects of cyber crimes.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code (U.S.C.) §§ 1030(a)(2)(C), 1030(a)(4), 2511(1)(a) and 2511(1)(d) have been committed by an unknown person or persons using the e-mail account smartinschurch091@gmail.com. There is also probable cause to search the above account, further described in Attachment A, for the items specified in Attachment B, which constitute evidence, instrumentalities, or fruits of the foregoing violations.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703 (c)(1)(A). Specifically, the United States District Court for the District of Montana is “a district court of the United States . . . that – has jurisdiction over the offense being investigated,” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND CONCERNING E-MAIL

6. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Google allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

7. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

8. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such

information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

9. In my training and experience, although the personal identifying information requested by an e-mail provider from a subscriber is not validated and can be easily falsified, the contents of e-mail communications can contain the subscribers true information, such as name, address, telephone number, and other email addresses and communications facilities used by a subscriber. Further, the contents of email messages can contain indentifying information of other unknown subjects and additional victims. The contents of emails can also hold written conversations between the subscriber and his/her contacts discussing activities related to the crimes under investigation. Therefore, in my training and experience, the information found in the contents of email messages may constitute evidences of the crimes under investigation, because such information can be used to identify subjects, accomplices, additional victims, and further details about the crimes under investigation such as motives and methods.

10. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP

address information can help to identify which computers or other devices were used to access the e-mail account.

11. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

BACKGROUND CONCERNING MICROSOFT EXCHANGE AND OUTLOOK

12. In my training and experience, I have learned that Microsoft Exchange is an e-mail system created by Microsoft to manage receipt, storage, and delivery of e-mail messages. Microsoft Outlook is an e-mail client application used to interact with Microsoft Exchange. Microsoft Outlook Web Access (OWA) is a web based version of Microsoft Outlook that allows a user to access their Microsoft Exchange e-mail account via a web browser, such as Internet Explorer or Mozilla Firefox, without having Microsoft Outlook installed on the computer they are using. A user or administrator can create automated instructions in Microsoft Exchange and Microsoft Outlook to handle incoming and outgoing email messages. These instructions are referred to as "rules." Rules created in Microsoft Outlook or OWA are referred to as "client-side rules" and rules created in Microsoft Exchange are referred to as "server-side rules." Rules can be created to automate a wide variety of actions including, but not limited to, placing all email

from a specific sender in a specific folder, forwarding all emails from a specific sender to a third-party email account, or deleting incoming messages from a specific sender.

BACKGROUND CONCERNING HOSTING PROVIDERS

13. In my training and experience, a hosting provider is a company that provides Internet-connected computer server resources to individuals or other companies. These server resources can be in the form of individual physical servers, often called dedicated servers, or they can be in the form of virtual servers, often referred to as Virtual Private Servers (VPS), which are servers created by using software to segment the resources of a physical server and isolating them to behave and function like multiple individual servers. A server leased from a hosting provider can be used for a variety of purposes, including hosting a website, storing electronic files, or acting as a proxy server.

BACKGROUND CONCERNING ANONYMOUS PROXY SERVICES

14. A proxy server is a computer that performs a given function in place of another computer. In my training and experience, Internet connections can be made from an originating computer to a destination computer through a proxy server, whereby the IP address of the originating computer remains hidden to the destination computer.

15. There are organizations who lease multiple servers from various hosting providers to form a network of proxies. These organizations then offer anonymous proxy services by supplying customers with an encrypted connection to their proxy network through which customers conduct their online activities. In my training and experience, anonymous proxy services allow customers to hide their true IP address whether they are sending emails, logging in to Internet accounts or browsing websites. Anonymous proxy service providers typically do not maintain any connection logs regarding the proxies their customers connect to. In my training

and experience, this makes it impossible to trace a customer's true originating IP address via historical methods, such as subpoenas or search warrants seeking records. In my training and experience, anonymous proxy services are popular among computer criminals, because their use severely impedes investigative efforts to attribute crimes on the Internet to those responsible.

SUBPOENA INFORMATION

16. On May 30, 2013, a grand jury subpoena was sent to Google, Inc. for email address smartinschurch091@gmail.com.

17. On July 17, 2013, Google, Inc. responded to the subpoena and provided subscriber information for smartinschurch091@gmail.com as follows:

18. Email address smartinschurch091@gmail.com was registered on May 17, 2012, from IP address 85.13.210.42. The subscriber registered the account using the name Sarah Potter and telephone number +447046362263, which is a mobile telephone number in the United Kingdom (UK). No physical address was provided by the subscriber. IP address 85.13.210.42 belongs to Coreix, Ltd., a hosting provider located in London, UK.

19. Google, Inc also provided login history for email address smartinschurch091@gmail.com, which showed logins from various IP address located in the UK, US, Canada and Nigeria, including US IP address 198.211.103.228 belonging to DigitalOcean. DigitalOcean is a VPS hosting provider located in New York, NY.

20. On July 2, 2013, a grand jury subpoena was served to DigitalOcean for a separate IP address 198.211.103.38, which was used to send emails to BEC from fraudulent email account kassandra.seedmaster@yahoo.ca, discussed further below.

21. On July 3, 2013, Digital Ocean responded to the subpoena and provided subscriber information for 198.211.103.38 showing the subscriber as TunnelBear, Inc.

(TunnelBear). TunnelBear is an anonymous proxy service provider located at 174 Spadina Avenue, Suite 206, Toronto, Ontario, Canada. This shows that the subscriber of kassandra.seedmaster@yahoo.ca used the TunnelBear service to send emails to BEC.

22. DigitalOcean, in accordance with the subpoena, also provided other facilities subscribed to by TunnelBear, Inc. including the above noted IP address 198.211.103.228, showing that the user of stmartinschurch091@gmail.com also used the TunnelBear service.

FACTS ESTABLISHING PROBABLE CAUSE

23. By way of background, Big Equipment Company, LLC (BEC) is a heavy equipment and farm machinery sales business owned by Ron Harmon and located in Havre, Montana. BEC is a business partner of Seedmaster, Inc. (Seedmaster); a heavy equipment and farm machinery manufacturer located in Emerald Park, Saskatchewan, Canada. BEC has customers located in the United States and Canada.

24. On March 4, 2013, Michael Sabine of Swift Current, Saskatchewan, Canada, purchased a piece of farm equipment from BEC for the agreed upon price of \$59,500 USD. Payment arrangements were made whereby Mr. Sabine would make payment via wire transfer directly to Seedmaster to avoid currency exchange issues from Canadian dollars to US dollars. BEC had an outstanding debt with Seedmaster against which Mr. Sabine's payment would be applied.

25. Details of the transaction were coordinated by BEC Accounts Manager Barb Fell, and Seedmaster Controller Kassandra Mohr. Communication between Ms. Fell and Ms. Mohr was conducted primarily via e-mail. Ms. Fell used e-mail account bigequip@bigequipment.com and Ms. Mohr used e-mail account kassandra@seedmaster.ca. During the course of coordinating Mr. Sabine's purchase and beginning on February 26, 2013, the e-mail messages between Ms.

Mohr and Ms. Fell began to be intercepted and modified by an unknown person or persons, and forwarded to the intended recipients via fraudulent e-mail accounts made to appear similar to the legitimate e-mail accounts above. Specifically, when Ms. Mohr sent e-mail to Ms. Fell from her legitimate e-mail account kassandra@seedmaster.ca, Ms. Fell would received the e-mail from kassandra.seedmaster@yahoo.ca, and when Ms. Fell sent e-mail to Ms. Mohr from her legitimate e-mail account bigequip@bigequipment.com, Ms. Mohr would receive the e-mail from barb.bigequipment@yahoo.com. Ms. Mohr did not register or subscribe to e-mail account kassandra.seedmaster@yahoo.ca and Ms. Fell did not register or subscribe to e-mail account barb.bigequipment@yahoo.com. Therefore, e-mail accounts kassandra.seedmaster@yahoo.ca and barb.bigequipment@yahoo.ca are fraudulent, and the person or persons using those account fraudulently impersonated Ms. Mohr and Ms. Fell.

26. On March 1, 2013, Ms. Fell received an e-mail from fraudulent account kassandra.seedmaster@yahoo.ca which contained wire transfer instructions and bank information for an account at NatWest Bank in the United Kingdom. Seedmaster does not maintain a bank account at NatWest Bank in the United Kingdom; therefore the wire transfer instructions were fraudulent. This e-mail message featured the same graphical logo and signature information as the e-mails Ms. Fell had received from kassandra@seedmaster.ca, causing it to appear like a legitimate e-mail from Ms. Mohr. Not realizing the information was fraudulent, Ms. Fell forwarded the fraudulent wire transfer information to Mr. Sabine's bank, Innovation Credit Union, who made payment of \$59,500 USD per the fraudulent instructions.

27. On May 9, 2013, your affiant examined Ms. Fell's work computer at BEC. Examination of the Microsoft Outlook settings for account bigequip@bigequipment.com on Ms. Fell's computer revealed two rules, visually represented in Attachment C, which had been

created to cause incoming e-mails from kassandra@seedmaster.ca to be redirected to two third-party e-mail accounts; fraudulent account barb.bigequipment@yahoo.com and heretofore unknown account stmartinschurch091@gmail.com. The rules then caused the incoming messages from kassndra@seedmaster.ca to be deleted from the inbox of barb@bigequipment.com so that Ms. Fell never saw the legitimate e-mail messages from Ms. Mohr. These two rules were not created by any employee of BEC, and did not serve any legitimate business purpose. Therefore, there is probable cause to believe these rules were created by a trespasser, and the forwarding email accounts barb.bigequipment@yahoo.com and stmartinschurch091@gmail.com are controlled by the trespasser.

28. The above described Microsoft Outlook rules configuration on Ms. Fell's computer resulted in all e-mails from kassandra@seedmaster.ca to bigequip@bigequipment.com being redirected to barb.bigequipment@yahoo.com and stmartinschurch@gmail.com instead of arriving at their intended destination. This is the mechanism by which a trespasser was able to intercept and modify e-mail communications between Ms. Mohr and Ms. Fell, and use those communications to perpetrate the above described fraud.

29. The above detailed subpoena results show that the user of stmartinschurch091@gmail.com and kassandra.seedmaster@yahoo.ca both used the TunnelBear service to conceal their true originating IP address. In addition, examination of the above detailed subpoena return from Google, and of the Internet headers of emails from kassandra.seedmaster@yahoo.ca to the victim, which the victim voluntarily provided, showed that some of the same IP addresses, namely 173.193.230.22, 205.204.85.89 and 184.107.23.250, were used to login to stmartinschurch091@gmail.com and kassandra.seedmaster@yahoo.ca.

30. IP address 173.193.230.22 pertains to SoftLayer Technologies located in Dallas, Texas, IP address 205.204.85.89 pertains to Netelligent Hosting located in Laval, Quebec, Canada, and IP address 184.107.23.250 pertains to iWeb Technologies located in Montreal, Quebec, Canada. All three of these entities are hosting service providers. This means that these three IP addresses do not reflect the true originating IP addresses of the person/s using smartinschurch091@gmail.com and kassandra.seedmaster@yahoo.ca, but rather represent connections through proxy servers. Because both accounts were accessed using the same proxy servers, there is probable cause to believe that e-mail account smartinschurch091@gmail.com is controlled by the same person/s that control kassandra.seedmaster@yahoo.ca, and is therefore related to the above described fraud.

31. On May 10, 2013, your affiant sent a preservation letter to Google Legal Investigations Support via facsimile to telephone number (650) 649-2939, requiring Google to preserve all records and contents of account smartinschurch091@gmail.com for a period of 90 days. On August 26, 2013, your affiant sent another preservation letter renewing preservation of said account. Therefore, it is reasonable to believe that the items sought, as described in Attachment B, are still in the possession of Google. In general, an e-mail that is sent to a Google e-mail (Gmail) subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for a certain period of time.

CONCLUSION

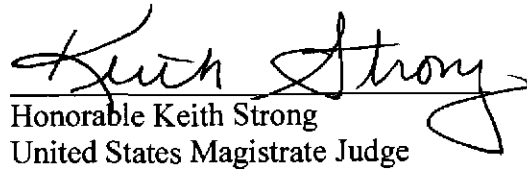
32. Based on the forgoing, I believe there is probable cause to believe that the information associated with email account smartinschurch091@gmail.com that is stored at

premises controlled by Google, Inc. contains evidence of violations of 18 U.S.C. §§
1030(a)(2)(C), 1030(a)(4), 2511(1)(a) and 2511(1)(d), as listed in Attachment B and described
above.



Shiloh A. Allen
Special Agent, Federal Bureau of Investigation
Great Falls, Montana

Subscribed and sworn before me this 3 day of October, 2013.



Honorable Keith Strong
United States Magistrate Judge